不使用双线性映射的无证书签密方案的安全性分析及改进

周彦伟[1),2),3)] 杨 波[1),2),3)] 张文政[2)]

[1)](陕西师范大学计算机科学学院 西安 710119)

[2)](保密通信重点实验室 成都 610041)

[3)](中国科学院信息工程研究所信息安全国家重点实验室 北京 100093)

摘 要 由于现有的基于双线性映射的无证书签密方案存在计算效率低的不足,因此一种不使用双线性映射的新的无证书签密方案由 Zhu 等人提出;同时,在随机谕言机模型中对该方案的安全性进行了证明. 该文通过构造具体的机密性和不可伪造性攻击算法,证明了 Zhu 等人所提出的方案无法满足其所声称的机密性和对$\mathcal{A}_I$类敌手的不可伪造性;针对上述问题,该文提出了安全高效的无证书签密方案,并在随机谕言机模型下基于计算性 Diffie-Hellman 困难问题和离散对数困难问题证明了该文所提方案的机密性和不可伪造性;相较于其他无证书签密方案,该文所提方案的安全性和计算效率更优.

关键词 无证书签密方案;随机谕言机模型;无双线性配对;离散对数;计算性 Diffie-Hellman;网络空间安全;信息安全

中图法分类号 TP393 **DOI 号** 10.11897/SP.J.1016.2016.01257

Security Analysis and Improvement of Certificateless Signcryption Scheme Without Bilinear Pairing

ZHOU Yan-Wei[1),2),3)] YANG Bo[1),2),3)] ZHANG Wen-Zheng[2)]

[1)](*School of Computer Science, Shaanxi Normal University, Xi'an* 710119)

[2)](*Science and Technology on Communication Security Laboratory, Chengdu* 610041)

[3)](*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093)

Abstract Almost all existing certificateless signcryption (CLS) schemes based on pairings have the shortcomings of low computational efficiency. Thus, based on discrete logarithm, a new CLS scheme without pairings was proposed by Zhu et al. It is provably secure in the Random Oracle Model (ROM). However, by giving concrete attacks about confidentiality and unforgeability, this study finds that the certificateless signcryption scheme proposed is not secure. Thus, based on Computational Diffie-Hellman (CDH) and Discrete Logarithm (DL), an efficient and security CLS scheme without pairings is proposed in this paper. It is provably secure in the ROM under the CDH and DL assumption. Moreover, compared with other existing CLS schemes in the computational complexity, the scheme without using pairings operation has more efficiency and security.

Keywords certificateless signcryption scheme; random oracle model; without pairings; discrete logarithm; computational Diffie-Hellman; cyberspace security; information security

收稿日期:2014-11-27;在线出版日期:2015-07-15. 本课题得到国家自然科学基金(61272436,61402275,61572303,61303092)、中国科学院信息工程研究所信息安全国家重点实验室开放课题(2015-MS-10)、保密通信重点实验室基金(9140C110206140C11050)、中央高校基本科研业务费专项资金(GK201504016)及陕西师范大学优秀博士论文项目(X2014YB01)资助.**周彦伟**,男,1986 年生,博士研究生,主要研究兴趣为密码学、无线网络通信技术等. E-mail: zyw_snnu@foxmail.com. **杨 波**(通信作者),男,1963 年生,博士,教授,博士生导师,陕西省"百人计划"特聘教授,主要研究领域为信息安全、密码学等. E-mail: byang@snnu.edu.cn. **张文政**,男,1966 年生,研究员,主要研究领域为信息安全等.

1 引 言

认证性和机密性是安全通信系统的基本要求，其中，消息的认证性通常由签名完成，而消息的机密性则通过加密来实现，然而传统的“先签名后加密”方式存在着计算效率低的不足；文献[1]首次提出了签密的概念，即在一个逻辑步骤内同时完成签名和加密操作，该机制具有计算成本和通信成本都比较低的优点，是数据信息较为理想的一种安全传输方法.

无证书公钥密码系统(CL-PKC)是由 Al-Riyami 和 Paterson 在文献[2]中提出的. 在 CL-PKC 中，用户基于密钥生成中心(Key Generation Center，KGC)为其计算出的部分私钥和随机选取的秘密值生成用户的完整私钥；公钥由用户的秘密值、身份信息和系统参数计算得出. CL-PKC 克服了公钥证书的管理问题，同时消除了用户密钥的托管问题[3]，提高了密码系统的运行效率.

自 Barbosa 等人[4]提出无证书签密的概念以来，关于无证书签密方案的研究已成为密码学领域当前的研究热点之一. 随着研究工作的逐渐深入，国内外众多学者分别提出了新的签密方案[4-12]. 文献[4]提出了一种使用双线性映射的无证书签密方案，该方案具有前向安全性，但未进行正式的安全性证明；文献[5]利用双线性映射构造了一种无证书签密方案，虽然，Sharmila 等人指出该方案在机密性上存在不足①，但是并未提出相应的改进方案；文献[6]在随机谕言机模型下对所提出的无证书签密机制进行了安全性证明，但该方案需要进行多次双线性映射运算. 虽然文献[4-6]分别提出了相应的无证书签密方案，但各方案中均使用双线性映射进行密钥的生成、签密计算或验证签密密文的合法性，各方案的运算量较大，都存在着计算效率低的不足；同时，部分方案也存在着安全性缺陷. 针对双线性映射计算复杂度较高的问题，不使用双线性映射的无证书签密方案[7-12]相继被人提出. 文献[7-8]分别提出了无需双线性映射的无证书签密方案，并在随机谕言机模型下基于计算性 Diffie-Hellman(Computational Diffie-Hellman，CDH)问题和离散对数(Discrete Logarithm，DL)问题的困难性对相应方案的机密性和不可伪造性进行了证明，同时对相应方案的执行效率进行了分析；文献[9]通过分析发现文献[8]无法满足其所声称的不可伪造性，并对该方案进行了改进；在文献[10-12]中分别提出了不使用双线性映射的无证书签密方案，并在随机谕言机模型下基于相应的困难性问题证明了各自方案的机密性和不可伪造性；文献[11]提出了不使用双线性映射的无证书代理签密机制，并分析了计算和通信效率以及安全性. 文献[7-12]均未使用双线性映射，一定程度上提高了方案的计算效率，但本文分析发现文献[11-12]中的点乘运算次数较多，导致计算效率依然较低；并且文献[7-10]的方案在安全性方面均存在缺陷；而文献[11]的密文长度较长，使得该方案的通信开销较大.

本文通过构造具体的不可伪造性和机密性攻击算法，证明了文献[7]的方案无法满足其所声称的对 $\mathcal{A}_I$ 类敌手的不可伪造性和对任意敌手的机密性；同时，指出文献[8-10]中的方案均不满足对任意敌手的机密性；并且通过分析发现文献[11-12]中的相关方案在计算效率方面存在一定的不足；遗憾的是文献[7-8]的方案没能满足其所声称的机密性和对 $\mathcal{A}_I$ 类敌手的不可伪造性，但上述方案新颖的设计思路，确实为不使用双线性映射运算的无证书签密方案的设计提供了新的设计思路.

针对上述问题，本文提出了无需进行双线性映射运算的安全高效的无证书签密方案，并在随机谕言机模型下基于 CDH 和 DL 假设证明了该方案的机密性和不可伪造性；相比于现有的无证书签密方案[4-12]，本文方案的安全性和计算效率更优.

2 预备知识

本节介绍 DL 假设、CDH 假设、无证书签密方案的基本构成算法和安全模型等相关基础知识.

2.1 相关困难性问题

离散对数(DL)问题：令 p 和 q 是满足条件 $p|q-1$ 的两个大素数，设 g 是群 Z_p^* 上阶为 q 的任意生成元，给定元组 $g, g^b \in Z_p^*$(其中 $b \in Z_q^*$ 且未知)，DL 问题的目的是计算 b.

算法 $\mathcal{A}$ 在概率多项式时间内成功解决 DL 问题的概率为 $Adv^{DL}(\mathcal{A}) = Pr[\mathcal{A}(g, g^b) = b]$.

其中概率来源于算法 $\mathcal{A}$ 的随机选择和 b 在 Z_q^* 上的随机选取.

① Sharmila D S, Vivek S S, Pandu R C. On the security of certificateless signcryption schemes. http://eprint.iacr.org/2009/298.pdf

定义 1.　DL 假设. 对于任意的概率多项式时间算法$\mathcal{A}$,优势 $Adv^{DL}(\mathcal{A})$是可忽略的.

计算性 Diffie-Hellman(CDH)问题:令 p 和 q 是满足条件 $p|q-1$ 的两个大素数,设 g 是群 Z_p^* 上阶为 q 的任意生成元,给定元组 $g,g^a,g^b\in Z_p^*$(其中 $a,b\in Z_q^*$ 且未知),CDH 的目的是证明 $g^{ab}\in Z_p^*$.

算法$\mathcal{A}$在概率多项式时间内成功解决 CDH 问题的概率为 $Adv^{CDH}(\mathcal{A})=Pr[\mathcal{A}(g,g^a,g^b)=g^{ab}]$.

其中概率来源于算法$\mathcal{A}$的随机选择和 a,b 在 Z_q^* 上的随机选取.

定义 2.　CDH 假设. 对于任意的概率多项式时间算法$\mathcal{A}$,优势 $Adv^{CDH}(\mathcal{A})$是可忽略的.

2.2　安全模型

根据文献[13]中的安全模型,本文将无证书签密方案的攻击敌手分为$\mathcal{A}_{\mathrm{I}}$和$\mathcal{A}_{\mathrm{II}}$两类.

$\mathcal{A}_{\mathrm{I}}$:此类敌手无法掌握系统的主密钥,但其具有替换合法用户公钥的能力,则$\mathcal{A}_{\mathrm{I}}$类敌手为恶意的用户. 本文中$\mathcal{A}_{\mathrm{I}\text{-}i}(i=1,2)$为$\mathcal{A}_{\mathrm{I}}$类敌手,其中$\mathcal{A}_{\mathrm{I}\text{-}1}$是攻击方案机密性的敌手,$\mathcal{A}_{\mathrm{I}\text{-}2}$是攻击方案不可伪造性的敌手.

$\mathcal{A}_{\mathrm{II}}$:此类敌手可掌握系统的主密钥,但其不具有替换合法用户公钥的能力,则$\mathcal{A}_{\mathrm{II}}$类敌手为恶意的 KGC. 本文中$\mathcal{A}_{\mathrm{II}\text{-}i}(i=1,2)$为$\mathcal{A}_{\mathrm{II}}$类敌手,其中$\mathcal{A}_{\mathrm{II}\text{-}1}$是攻击方案机密性的敌手,$\mathcal{A}_{\mathrm{II}\text{-}2}$是攻击方案不可伪造性的敌手.

文献[7,13]详细地介绍了无证书签密方案在$\mathcal{A}_{\mathrm{I}}$和$\mathcal{A}_{\mathrm{II}}$两类敌手适应性地选择消息攻击下不可伪造性和适应性地选择密文攻击下机密性的定义及相应的游戏,本文不再赘述,安全模型及游戏的具体定义详见文献[7,13].

3　Zhu 等人方案的安全性分析

本节构造具体的不可伪造性和机密性攻击算法,证明文献[7]中的方案无法满足其声称的不可伪造性和机密性.

3.1　不可伪造性攻击

令用户 Alice 和 Bob 分别为文献[7]方案中的发送者和接收者,则 Alice 和 Bob 的公私钥对分别为$\langle PK_a=(w_a,u_a),SK_a=(t_a,z_a)\rangle$和$\langle PK_b=(w_b,u_b),SK_b=(t_b,z_b)\rangle$.

$\mathcal{A}_{\mathrm{I}}$类敌手 Dave(Dave 为攻击方案不可伪造性的敌手)在掌握 Alice 的公钥 $PK_a=(w_a,u_a)$后,使用伪造公钥替代 Alice 的公钥去生成合法的伪造签密密文.

敌手 Dave 与 Bob 间的消息交互过程如下所示:

(1)敌手 Dave 伪造 Alice 的公钥

① Dave 掌握 Alice 的公钥 $PK_a=(w_a,u_a)$和身份标识 ID_a等公开信息后,基于上述公开信息计算部分伪造公钥 $u_a'=(w_a y^{H_1(ID_a,w_a)})^{-1}$;

② Dave 使用伪造公钥$PK_a'=(w_a,u_a')$代替Alice的原始公钥 $PK_a=(w_a,u_a)$,此时 Bob 将认为 Alice 的公钥就为 $PK_a'=(w_a,u_a')$.

(2)敌手 Dave 伪造 Alice 的签密密文

Dave 随机选取秘密数 $r\in Z_q^*$,首先计算 $R=g^r$;然后计算 $h_1=H_1(ID_b,w_b)$,$h'=H_2(ID_a,R,m)$;最后计算 $S'=r(h')^{-1}$,$C'=H_3(u_b w_b y^{h_1})^r\oplus m$. 发送密文消息 $\sigma'=(h',S',C')$给 Bob.

(3)Bob 验证签密密文的合法性

Bob 收到密文 σ'后,对 σ'进行解签密验证. 若验证证明密文 σ'是合法密文,则 Dave 伪造了 Alice 的合法签密密文,即 Dave 伪造成功;否则,Dave 伪造失败.

定理 1.　$\mathcal{A}_{\mathrm{I}}$类敌手 Dave 伪造了 Alice 的合法签密密文.

证明.　Bob 收到签密密文 $\sigma'=(h',S',C')$后,密文的合法性验证过程如下:

① 计算 $h_1'=H_1(ID_a,w_a)$;

② 计算 $V'=(u_a' w_a y^{h_1'} g^{h'})^{S'(Z_b+t_b)}$,恢复消息 $m'=H_3(V')\oplus C'$;

由于 $u_a' w_a y^{h_1'} g^{h'}=(w_a y^{H_1(ID_a,w_a)})^{-1} w_a y^{h_1'} g^{h'}=(w_a y^{H_1(ID_a,w_a)})^{-1} w_a y^{H_1(ID_a,w_a)} g^{h'}=g^{h'}$;

则有 $V'=(u_a' w_a y^{h_1'} g^{h'})^{S'(z_b+t_b)}=(g^{h'})^{S'(z_b+t_b)}=g^{r(z_b+t_b)}=g^{r(z_b+s_b+xh_1)}$;$(u_b w_b y^{h_1})^r=g^{r(z_b+s_b+xh_1)}$(其中 $h_1=H_1(ID_b,w_b)$);

由上述计算可知

$$m'=m \tag{1}$$

③ 验证 $h'=H_2(ID_a,(u_a' w_a y^{h_1'} g^{h'})^{S'},m')$是否成立,若等式成立,则 Bob 认为签密 σ'是由 Alice 生成的合法签密密文.

由于$(u_a' w_a y^{h_1'} g^{h'})^{S'}=g^{h'S'}=g^r=R$;

则有

$$h'=H_2(ID_a,(u_a' w_a y^{h_1'} g^{h'})^{S'},m') \tag{2}$$

由等式(1)和(2)可知,伪造密文 σ'通过了密文接收者 Bob 的合法性验证,则$\mathcal{A}_{\mathrm{I}}$类敌手 Dave 具有伪造 Alice 合法签密密文的能力.

在验证密文合法性时，参数 h_1' 由 ID_a 和 w_a 通过哈希计算等到，部分公钥 z_a 与 h_1' 之间未形成一一对应的关系，即对 z_a 的改变并未对参数 h_1' 造成影响，则 $\mathcal{A}_I$ 类敌手可根据验证等式构造替代公钥，完成不可伪造性攻击.

3.2 机密性攻击

设敌手 Smart 是 $\mathcal{A}_I$ 或 $\mathcal{A}_{II}$ 类敌手(Smart 为攻击方案机密性的敌手). 由文献[7]中游戏 1 和 2 可知：Smart 向谕言机发送的挑战信息包括：两个等长的消息 $\{m_0, m_1\}$ 和两个身份标识 $\{ID_S, ID_V\}$，其中不能对 ID_V 执行部分密钥提取询问或私钥提取询问. 但在挑战阶段，Smart 可询问谕言机获知 ID_S 的公钥 $PK_S=(w_S, u_S)$.

谕言机收到 Smart 的签密询问后，随机选取 $b\in\{0,1\}$，并生成 m_b 的挑战密文 $\sigma^*=(h^*, S^*, C^*)$，当 Smart 收到谕言机的挑战密文 σ^* 后，Smart 首先对 b 做出猜测，令 $b=0$，然后验证等式(3)是否成立，若成立则说明消息 m_0 是挑战密文 σ^* 所对应的明文，否则 m_1 是 σ^* 所相对应的明文.

$$h^*=H_2(ID_S, (u_S w_S y^{h_1} g^{h^*})^{S^*}, m_0) \tag{3}$$

其中公开参数 $y=g^x$，$h_1=H_1(ID_S, w_S)$.

由此可见文献[7]方案对 $\mathcal{A}_I$ 和 $\mathcal{A}_{II}$ 类敌手均不具有密文机密性. 使用上述机密性攻击算法同样可证明文献[8-10]中的方案均无法满足其所声称的对任意敌手的机密性.

密文的合法性验证过程中的相关参数均为发送者的公开信息，即明文 m 与部分密文 h 之间形成了对应关系，因此敌手可通过尝试验证的策略完成机密性攻击.

4 本文签密方案

4.1 方案描述

本节提出了安全高效的无证书签密方案，具体细节描述如下：

(1) 系统建立阶段($Setup$)

系统初始化阶段，KGC 进行如下操作：

① 输入安全参数 k，输出满足条件 $p|q-1$ 的两个大素数 p 和 q. g 为群 Z_p^* 中任意阶为 q 的生成元；

② 定义抗碰撞的安全哈希函数：$H_1:\{0,1\}^{L_1}\times Z_p^*\times Z_p^*\to Z_q^*$，$H_2:\{0,1\}^{L_1}\times\{0,1\}^{L_2}\times Z_p^*\to Z_q^*$，$H_3:Z_p^*\to\{0,1\}^{L_2+|Z_q^*|}$，$H_4:\{0,1\}^{L_1}\times\{0,1\}^{L_2}\times Z_p^*\times Z_p^*\to Z_q^*$，其中 L_1 为用户身份标识 ID 的长度，L_2 为明文消息的长度，$|Z_q^*|$ 为 Z_q^* 中元素的长度；

③ 定义“$\oplus$”为异或运算，“$\|$”为连接符；

④ 随机选取系统主密钥 $s\in Z_q^*$，计算 $P_{Pub}=g^s$；公开 $Params=\langle p, q, Z_p^*, g, P_{Pub}, H_1, H_2, H_3, H_4, \oplus, \|\rangle$，秘密保存主密钥 s.

(2) 用户密钥生成($KeyExtract$)

用户 ID_i 的密钥生成过程如下所述：

① 随机选取秘密值 $x_i\in Z_q^*$，计算 $X_i=g^{x_i}$，发送身份标识 ID_i 和公开参数 X_i 给 KGC；

② 给定用户身份标识 ID_i 及公开参数 X_i，KGC 随机选取秘密数 $r_i\in Z_q^*$，分别计算 $Y_i=g^{r_i}$ 和 $y_i=r_i+sH_1(ID_i, X_i, Y_i)$，通过安全信道将 y_i 和 Y_i 返回给用户 ID_i，其中 y_i 为用户的部分私钥，Y_i 为用户的部分公钥. 因此，用户 ID_i 的公私钥对为 $\langle PK_i=(X_i, Y_i), SK_i=(x_i, y_i)\rangle$.

设本文签密密文发送者 Alice(其身份标识为 ID_a)和密文接收者 Bob(其身份标识为 ID_b)的公私钥对分别为 $\langle PK_A=(X_a, Y_a), SK_A=(x_a, y_a)\rangle$ 和 $\langle PK_B=(X_b, Y_b), SK_B=(x_b, y_b)\rangle$.

Alice 和 Bob 通过等式 $g^{y_a}=Y_a P_{Pub}^{H_1(ID_a, X_a, Y_a)}$ 和 $g^{y_b}=Y_b P_{Pub}^{H_1(ID_b, X_b, Y_b)}$ 验证 KGC 生成的部分私钥和部分公钥的正确性.

(3) 签密($Signcrypt$)

若发送消息 m 给 Bob，Alice 则进行下述操作.

① 随机选取秘密数 $a\in Z_q^*$，计算 $R=g^a$；

② 计算 $h_1^B=H_1(ID_b, X_b, Y_b)$，$V=(X_b Y_b P_{Pub}^{h_1^B})^a$ 和 $U=d(x_a+y_a)+af$(其中 $d=H_4(ID_a, m, X_a, R)$，$f=H_4(ID_a, m, Y_a, R)$)；

③ 生成签密密文 $C=(m\|U)\oplus H_3(V)$，$h=H_2(ID_a, R, C)$ 和 $S=a(x_a+y_a+h)^{-1}$；

④ 发送签密密文 $\sigma=(h, S, C)$ 给接收者 Bob.

(4) 签密验证($UnSigncrypt$)

收到密文 $\sigma=(h, S, C)$ 后，Bob 进行下述操作.

① 计算 $h_1^A=H_1(ID_a, X_a, Y_a)$，$R'=(X_a Y_a P_{Pub}^{h_1^A} g^h)^S$ 和 $V'=R'^{(x_b+y_b)}$；

② 恢复明文消息 $m\|U=C\oplus H_3(V')$；

③ 验证等式 $g^U=(X_a Y_a P_{Pub}^{h_1^A})^{d'} R'^{f'}$(其中 $d'=H_4(ID_a, m, X_a, R')$，$f'=H_4(ID_a, m, Y_a, R')$)和 $h=H_2(ID_a, R', C)$ 是否成立，若等式成立，则接收消息 m；否则输出 $\perp$.

4.2 正确性

定理 2. 密文接收者可以从密文消息 $\sigma=(h,S,C)$ 中恢复出原始的明文消息，并且能验证发送者身份的合法性.

证明. Bob 的密文解密过程如下所述：

① 计算

$$V'=(g^{x_a}g^{r_a}g^{sh_1^A}g^h)^{S(x_b+y_b)}$$
$$=g^{(x_a+r_a+sh_1^A+h)a(x_a+y_a+h)^{-1}(x_b+y_b)}=g^{a(x_b+y_b)},$$

其中，$h_1^A=H_1(ID_a,X_a,Y_a)$ 和 $y_a=r_a+sh_1^A$；

② 计算

$$V=(g^{x_b}g^{r_b}g^{sh_1^B})^a=g^{(x_b+r_b+sh_1^B)a}=g^{a(x_b+y_b)},$$

其中，$h_1^B=H_1(ID_b,X_b,Y_b)$ 和 $y_b=r_b+sh_1^B$；

③ 因此 $m\parallel U=(m\parallel U)\oplus H_3(V)\oplus H_3(V')$，其中 $V=V'$.

因此，密文接收者能够基于发送者公钥还原出原始的通信消息，同时验证消息发送者的身份. 证毕.

定理 3. 密文接收者能够验证签名的合法性.

证明. Bob 的签名合法性验证过程如下所述：

① 计算

$$R'=(X_aY_aP_{Pub}^{h_1^A}g^h)^S=(g^{x_a}g^{r_a}g^{sh_1^A}g^h)^S$$
$$=g^{(x_a+r_a+sh_1^A+h)a(x_a+y_a+h)^{-1}}=g^a=R;$$

② 计算

$$g^U=g^{d(x_a+y_a)+af}=g^{d(x_a+y_a)}g^{af}=g^{d(x_a+r_a+sh_1^A)}g^{af}$$
$$=(X_aY_aP_{Pub}^{h_1^A})^dR^f=(X_aY_aP_{Pub}^{h_1^A})^{d'}R'^{f'},$$

其中，$R'=R$，$d'=H_4(ID_a,m,X_a,R')=d$，$f'=H_4(ID_a,m,Y_a,R')=f$.

③ 则有等式 $g^U=(X_aY_aP_{Pub}^{h_1^A})^{d'}R'^{f'}$ 和 $h=H_2(ID_a,R',C)$ 成立.

因此，Bob 能够验证签名的正确性，即 Bob 能够完成对密文 σ 的合法性及完整性的验证. 证毕.

5 安全性分析

5.1 机密性

定理 4. $\mathcal{A}_I$ 类敌手的机密性. 在随机谕言机模型中，若敌手 $\mathcal{A}_{I\text{-}1}$ 能以不可忽略的优势 ε 在多项式时间内赢得相关游戏（游戏具体定义详见文献[7]，$\mathcal{A}_{I\text{-}1}$ 最多进行 q_S 次签密询问和 q_{Sk} 次私钥生成询问），则算法 $\mathcal{F}$ 能以不可忽略的优势 $Adv(\mathcal{F})\geq\left(1-\frac{q_{SK}}{2^k}\right)^2\frac{\varepsilon}{e(q_S+1)}$（e 是自然对数底数）在多项式时间内解决 CDH 困难问题.

证明. 令算法 $\mathcal{F}$ 是输入为三元组 $\langle g,g^a,g^b\rangle$（其中 $a,b\in Z_q^*$ 且未知）的 CDH 问题解决者，其目的是证明 $g^{ab}\in Z_p^*$. $\mathcal{F}$ 以敌手 $\mathcal{A}_{I\text{-}1}$ 作为子程序并充当游戏的挑战者. $\mathcal{F}$ 运行 *Setup* 算法，并发送系统公开参数 $Params=\langle p,q,Z_p^*,g,P_{Pub},H_1,H_2,H_3,H_4\rangle$ 给 $\mathcal{A}_{I\text{-}1}$，其中令 $P_{Pub}=g^b$（系统主密钥为 b，但 $\mathcal{F}$ 并不掌握）；维持列表 $L_1,L_2,L_3,L_4,L_{SK},L_{PK}$ 用于跟踪 $\mathcal{A}_{I\text{-}1}$ 对谕言机 H_1,H_2,H_3,H_4 的询问以及对私钥生成和公钥生成的询问，初始时各列表均为空.

询问：敌手 $\mathcal{A}_{I\text{-}1}$ 进行下述询问.

H_2 询问：当 $\mathcal{F}$ 收到 $\mathcal{A}_{I\text{-}1}$ 对 H_2 的询问 $\langle ID_i,R_i,C_i\rangle$ 时，若存在 $\langle ID_i,R_i,C_i,h_2\rangle\in L_2$，则返回相应的 h_2 给 $\mathcal{A}_{I\text{-}1}$；否则，$\mathcal{F}$ 选取满足条件为 $\langle *,*,*,h_2\rangle\notin L_2$（避免碰撞的产生）的随机数 $h_2\in Z_q^*$，添加 $\langle ID_i,R_i,C_i,h_2\rangle$ 到 L_2 中，并返回 h_2 给 $\mathcal{A}_{I\text{-}1}$.

H_3 询问：当 $\mathcal{F}$ 收到 $\mathcal{A}_{I\text{-}1}$ 对 H_3 的询问 $\langle V_i\rangle$ 时，若存在 $\langle V_i,h_3\rangle\in L_3$，则返回相应的 h_3 给 $\mathcal{A}_{I\text{-}1}$；否则，$\mathcal{F}$ 选取满足 $\langle *,h_3\rangle\notin L_3$ 的随机数 $h_3\in\{0,1\}^{L_2+|Z_q^*|}$，添加 $\langle V_i,h_3\rangle$ 到 L_3 中，并返回 h_3 给 $\mathcal{A}_{I\text{-}1}$.

H_4 询问：当 $\mathcal{F}$ 收到 $\mathcal{A}_{I\text{-}1}$ 对 H_4 的询问 $\langle ID_i,m_i,X_i(Y_i),R_i\rangle$ 时，若 $\langle ID_i,m_i,X_i(Y_i),R_i,h_4\rangle\in L_4$，则返回 h_4 给 $\mathcal{A}_{I\text{-}1}$；否则 $\mathcal{F}$ 选取满足 $\langle *,*,*,*,h_4\rangle\notin L_4$ 的随机数 $h_4\in Z_q^*$，添加 $\langle ID_i,m_i,X_i(Y_i),R_i,h_4\rangle$ 到 L_4 中，并返回 h_4 给 $\mathcal{A}_{I\text{-}1}$.

公钥生成询问：当 $\mathcal{F}$ 收到 $\mathcal{A}_{I\text{-}1}$ 对 ID_i 的公钥生成询问时，$\mathcal{F}$ 进行下述操作.

① 若存在 $\langle ID_i,X_i,Y_i,c_i\rangle\in L_{PK}$，则返回元组中相应的公钥 $PK_i=\langle X_i,Y_i\rangle$ 给 $\mathcal{A}_{I\text{-}1}$；

② 否则，$\mathcal{F}$ 选取随机数 $c_i\leftarrow\{0,1\}$，且 $Pr[c_i=1]=\delta$ 且 $\delta=\frac{1}{q_S+1}$；若 $c_i=0$，$\mathcal{F}$ 选取满足 $\langle *,X_i,Y_i,*\rangle\notin L_{PK}$（其中 $X_i=g^{x_i}$ 和 $Y_i=g^{y_i}P_{Pub}^{-h_1}$）的随机数 $x_i,y_i,h_1\in Z_q^*$，添加 $\langle ID_i,X_i,Y_i,c_i\rangle$ 到 L_{PK} 中，返回 $PK_i=\langle X_i,Y_i\rangle$ 给 $\mathcal{A}_{I\text{-}1}$；同时，添加 $\langle ID_i,x_i,y_i\rangle$ 到 L_{SK} 中，添加 $\langle ID_i,X_i,Y_i,h_1\rangle$ 到 L_1 中；若 $c_i=1$，则令 $X_i=g^{r_{Know}^1}$ 和 $Y_i=g^{r_{Know}^2}$（$r_{Know}^1\in Z_p^*$ 和 $r_{Know}^2\in Z_p^*$ 为 $\mathcal{F}$ 已知的参数），且满足 $\langle *,X_i,Y_i,*\rangle\notin L_{PK}$，选取满足条件为 $\langle *,r_{Know}^1,y_i,*\rangle\notin L_{SK}$，$\langle *,*,*,h_1\rangle\notin L_1$ 和 $Y_i=g^{y_i}P_{Pub}^{-h_1}$ 的随机数 $y_i,h_1\in Z_q^*$，添加 $\langle ID_i,X_i,Y_i,c_i\rangle$ 到 L_{PK} 中，返回 $PK_i=\langle X_i,Y_i\rangle$ 给 $\mathcal{A}_{I\text{-}1}$，同时，添加 $\langle ID_i,x_i,y_i\rangle$ 到 L_{SK} 中，添加 $\langle ID_i,X_i,Y_i,h_1\rangle$ 到 L_1 中.

H_1 询问：当 $\mathcal{F}$ 收到 $\mathcal{A}_{I\text{-}1}$ 对 H_1 的询问 $\langle ID_i,X_i,Y_i\rangle$ 时，若存在 $\langle ID_i,X_i,Y_i,h_1\rangle\in L_1$，则返回相应的

h_1给$\mathcal{A}_{\text{I-1}}$；否则，$\mathcal{A}_{\text{I-1}}$对 ID_i进行公钥生成询问后，返回 L_1中相应元组的 h_1给$\mathcal{A}_{\text{I-1}}$.

私钥生成询问：当$\mathcal{F}$收到$\mathcal{A}_{\text{I-1}}$对 ID_i的私钥生成询问时，$\mathcal{F}$进行下述操作：

① 若存在$\langle ID_i, x_i, y_i\rangle \in L_{SK}$，则返回相应的私钥 $SK_i=\langle x_i, y_i\rangle$给$\mathcal{A}_{\text{I-1}}$；

② 否则，对 ID_i进行公钥生成询问后，在 L_{SK}中查找相应的元组$\langle ID_i, x_i, y_i\rangle$，并返回相应的私钥 $SK_i=\langle x_i, y_i\rangle$给$\mathcal{A}_{\text{I-1}}$.

公钥替换：$\mathcal{A}_{\text{I-1}}$可选择一个新的公钥 $PK_i'=\langle X_i', Y_i'\rangle$替换合法用户 ID_i的原始公钥 PK_i.

签密询问：当$\mathcal{F}$收到敌手$\mathcal{A}_{\text{I-1}}$对三元组$\langle ID_S, ID_R, m\rangle$（$\mathcal{A}_{\text{I-1}}$对 ID_S已进行了公钥生成询问）的签密询问时，$\mathcal{F}$在 L_{PK}中查询 ID_S对应的元组$\langle ID_S, X_S, Y_S, c_S\rangle$，并进行下述操作：

① 若 $c_S=1$，则$\mathcal{F}$结束，并终止模拟；

② 否则，$\mathcal{F}$在 L_{SK}与 L_{PK}中分别查询 ID_S及 ID_R对应的元组$\langle ID_S, x_S, y_S\rangle$和$\langle ID_R, X_R, Y_R\rangle$，运行算法 $Signcrypt(Params, ID_S, SK_S, ID_R, PK_R, m)$生成相应的密文 $\sigma=(h, S, C)$，并将 σ返回给$\mathcal{A}_{\text{I-1}}$.

解签密询问：当$\mathcal{F}$收到$\mathcal{A}_{\text{I-1}}$对元组$\langle ID_S, ID_R, \sigma=(h, S, C)\rangle$（$\mathcal{A}_{\text{I-1}}$对 ID_R已进行了公钥生成询问）的解签密询问时，$\mathcal{F}$在 L_{PK}中查询 ID_R所对应的元组$\langle ID_R, X_R, Y_R, c_R\rangle$，并进行下述操作：

① 若$\langle ID_R, X_R, Y_R, c_R\rangle \in L_{PK}$且 $c_R=0$，$\mathcal{F}$则分别在 L_{SK}与 L_{PK}中查询 ID_R及 ID_S相对应的元组$\langle ID_R, x_R, y_R\rangle$和$\langle ID_S, X_S, Y_S\rangle$，对密文 σ运行解签密算法 $UnSigncrypt(Params, ID_S, PK_S, ID_R, SK_R, \sigma)$，并返回 m给$\mathcal{A}_{\text{I-1}}$，若输入的密文无效，$\mathcal{F}$则终止模拟；

② 若$\langle ID_R, X_R, Y_R, c_R\rangle \in L_{PK}$且 $c_R=1$，当$\langle ID_S, X_S, Y_S, h_1\rangle \in L_1$，$\langle ID_S, R_S, C, h_2\rangle \in L_2$，$\langle V_i=g^{a(x_R+y_R)}, h_3\rangle \in L_3$，$\langle ID_S, m_S, X_S, R_S, h_4^X\rangle \in L_4$和$\langle ID_S, m_S, Y_S, R_S, h_4^Y\rangle \in L_4$，计算 $m \| U=C\oplus h_3$，若等式 $g^U=(X_S Y_S P_{Pub}^{h_1})^{h_4^X} R_S^{h_4^Y}$成立，则返回 m给$\mathcal{A}_{\text{I-1}}$，否则$\mathcal{F}$终止模拟；

③ 若列表 L_{PK}中不存在元组$\langle ID_S, X_S, Y_S\rangle$（即公钥被替换），当$\langle ID_S, X_S', Y_S', h_1\rangle \in L_1$，$\langle ID_S, R_S, C, h_2\rangle \in L_2$，$\langle V_i=g^{a(x_R+y_R)}, h_3\rangle \in L_3$，$\langle ID_S, m_S, X_S', R_S, h_4^X\rangle \in L_4$和$\langle ID_S, m_S, Y_S', R_S, h_4^Y\rangle \in L_4$，计算 $m \| U=C\oplus h_3$，若等式 $g^U=(X_S' Y_S' P_{Pub}^{h_1})^{h_4^X} R_S^{h_4^Y}$成立，则返回 m给$\mathcal{A}_{\text{I-1}}$，否则$\mathcal{F}$终止模拟.

挑战$\mathcal{A}_{\text{I-1}}$输出两个希望挑战的身份(ID_S, ID_R)和两个等长的明文(m_0, m_1).

收到$\mathcal{A}_{\text{I-1}}$的挑战信息后，由于$\mathcal{F}$对 ID_R已经进行了公钥密钥生成询问，$\mathcal{F}$可获得其在列表 L_{PK}中对应的元组$\langle ID_R, X_R, Y_R, c_R\rangle$，并进行下述操作.

① 若 $c_R=0$，则$\mathcal{F}$结束，并终止模拟；

② 否则，随机选取 $c\leftarrow\{0,1\}$，令 $R^*=g^a$，$\mathcal{F}$选取满足等式 $g^{U^*}=(X_S Y_S P_{Pub}^{h_1^S})^{d'} R^{*f'}$（其中 $d'=H_4(ID_S, m_c, X_S, R^*)$，$f'=H_4(ID_S, m_c, Y_S, R^*)$）的随机数 $U^*\in Z_q^*$；选取满足等式 $V^*=R^{*(x_R+y_R)}$的随机数 $V^*\in Z_p^*$；计算 $C^*=(m_c \| U^*)\oplus H_3(V^*)$和 $h^*=H_2(ID_S, R^*, C^*)$；选择满足 $R^*=(X_S Y_S P_{Pub}^{h_1^S} g^{h^*})^{S^*}$的随机数 $S^*\in Z_p^*$；发送 $\sigma^*=(h^*, S^*, C^*)$给$\mathcal{A}_{\text{I-1}}$.

$\mathcal{A}_{\text{I-1}}$经过概率多项式时间次数的上述询问后输出对 c的猜测 $c'\leftarrow\{0,1\}$，若 $c'=c$，$\mathcal{F}$输出 $g^{ab}=(V^* R^{*-(r_{Know}^1+r_{Know}^2)})^{(h_1^R)^{-1}}$作为 CDH 问题的有效解；否则，$\mathcal{F}$没有解决 CDH 问题.

$\mathcal{F}$为$\mathcal{A}_{\text{I-1}}$模拟了真实的攻击环境，若$\mathcal{F}$在模拟过程中未终止，并且$\mathcal{A}_{\text{I-1}}$以不可忽略的优势 ε攻破了本文方案的机密性，则$\mathcal{F}$输出 CDH 问题的有效解.

令事件$\mathcal{E}$表示$\mathcal{A}_{\text{I-1}}$对挑战身份 ID_S和 ID_R未进行私钥生成询问，即 $Pr[\mathcal{E}]=\left(1-\frac{q_{SK}}{2^k}\right)^2$，事件$\mathcal{E}_1$表示询问阶段$\mathcal{F}$未终止，即 $Pr[\mathcal{E}_1]=(1-\delta)^{q_S}$，事件$\mathcal{E}_2$表示挑战阶段$\mathcal{F}$未终止，即 $Pr[\mathcal{E}_2]=\delta$；则模拟过程中$\mathcal{F}$不终止的概率为 $Pr[\mathcal{E}\wedge\mathcal{E}_1\wedge\mathcal{E}_2]=\left(1-\frac{q_{SK}}{2^k}\right)^2\cdot(1-\delta)^{q_S}\delta$. 由于 $\delta=\frac{1}{q_S+1}$，当 q_S足够大时，$(1-\delta)^{q_S}$趋向于 e^{-1}（e 是自然对数底数），因此，模拟过程中$\mathcal{F}$不终止的概率至少为 $\left(1-\frac{q_{SK}}{2^k}\right)^2\frac{1}{e(q_S+1)}$.

综上所述，若$\mathcal{F}$在模拟过程中未终止，且$\mathcal{A}_{\text{I-1}}$以不可忽略的优势 ε攻破了本文签密方案的机密性，则$\mathcal{F}$能以优势 $Adv(\mathcal{F})\geq\left(1-\frac{q_{SK}}{2^k}\right)^2\frac{\varepsilon}{e(q_S+1)}$输出 CDH 问题的有效解. 证毕.

定理 5. $\mathcal{A}_{\text{II}}$类敌手的机密性. 在随机谕言机模型中，若敌手$\mathcal{A}_{\text{II-1}}$能以不可忽略的优势 ε在多项式时间内赢得相关游戏（游戏具体定义详见文献[7]），$\mathcal{A}_{\text{II-1}}$最多进行 q_S次签密询问和 q_{SK}次私钥生成询问），算法$\mathcal{F}$则能以不可忽略的优势 $Adv(\mathcal{F})\geq\left(1-\frac{q_{SK}}{2^k}\right)^2\frac{\varepsilon}{e(q_S+1)}$（e 是自然对数底数）在多项式时间内解决 CDH 困难问题.

证明思路与定理 4 相似，不再赘述.

5.2 不可伪造性

定理 6. $\mathcal{A}_{\mathrm{I}}$类敌手的不可伪造性. 在随机谕言机模型中，若敌手$\mathcal{A}_{\mathrm{I\text{-}2}}$能以不可忽略的优势 ε 在多项式时间内赢得相关游戏(游戏具体定义详见文献[7])，$\mathcal{A}_{\mathrm{I\text{-}2}}$最多进行 q_S次签密询问和 q_{SK}次私钥生成询问)，算法$\mathcal{F}$则能以不可忽略的优势 $Adv(\mathcal{F})\geq\left(1-\frac{q_{SK}}{2^k}\right)\frac{\varepsilon}{\mathrm{e}(q_S+1)}$(e 是自然对数底数)在多项式时间内解决 DL 困难问题.

证明. 令算法$\mathcal{F}$是输入为二元组$\langle g,g^b\rangle$(其中$b\in Z_q^*$且未知)的 DL 困难问题解决者，其目的是证明$b\in Z_q^*$. $\mathcal{F}$以敌手$\mathcal{A}_{\mathrm{I\text{-}2}}$作为子程序并充当游戏的挑战者. $\mathcal{F}$运行 $Setup$ 算法，并发送系统公开参数 $Params=\langle p,q,Z_p^*,g,P_{Pub},H_1,H_2,H_3,H_4\rangle$给$\mathcal{A}_{\mathrm{I\text{-}2}}$，令 $P_{Pub}=g^b$，维持列表 $L_1,L_2,L_3,L_4,L_{SK},L_{PK}$分别用于跟踪$\mathcal{A}_{\mathrm{I\text{-}2}}$对谕言机 H_1,H_2,H_3,H_4的询问以及对私钥生成和公钥生成的询问，初始时各列表均为空.

询问：敌手$\mathcal{A}_{\mathrm{I\text{-}2}}$执行定理 4 中对谕言机 H_1,H_2,H_4的询问、公钥生成询问、私钥生成询问和公钥替换询问.

签名询问：当$\mathcal{F}$收到$\mathcal{A}_{\mathrm{I\text{-}2}}$关于$(m,ID_S)$(敌手$\mathcal{A}_{\mathrm{I\text{-}2}}$对$ID_S$已进行了公钥生成询问)的签名询问时，$\mathcal{F}$先在列表 L_{PK}中查询ID_S所对应的元组$\langle ID_S,X_S,Y_S,c_S\rangle$：

① 若 $c_S=1$，则$\mathcal{F}$放弃，并终止模拟；

② 否则，$\mathcal{F}$在 L_{SK}中查询 ID_S对应的元组$\langle ID_S,x_S,y_S\rangle$，运行算法 $Sign(Params,ID_S,SK_S,m)$生成相应的签名 $\sigma=(h,S,U,m)$，并将其发送给$\mathcal{A}_{\mathrm{I\text{-}2}}$.

签名验证询问：当$\mathcal{F}$收到$\mathcal{A}_{\mathrm{I\text{-}2}}$对$\langle ID_S,\sigma=(h,S,U,m)\rangle$(敌手$\mathcal{A}_{\mathrm{I\text{-}2}}$对 ID_S已进行了公钥生成询问)的解签密询问时，$\mathcal{F}$在列表 L_{PK}中查询 ID_S所对应的元组$\langle ID_S,X_S,Y_S,c_S\rangle$：

①若$\langle ID_S,X_S,Y_S,c_S\rangle\in L_{PK}$且$c_S=0$，$\mathcal{F}$则运行算法 $UnSign(Params,ID_S,PK_S,\sigma)$，并返回 m 给$\mathcal{A}_{\mathrm{I\text{-}2}}$，若输入的签名无效，$\mathcal{F}$则终止模拟；

②若$\langle ID_S,X_S,Y_S,c_S\rangle\in L_{PK}$且$c_S=1$，当$\langle ID_S,X_S,Y_S,h_1\rangle\in L_1$，$\langle ID_S,R_S,C,h_2\rangle\in L_2$，$\langle ID_S,m_S,X_S,R_S,h_4^X\rangle\in L_4$和$\langle ID_S,m_S,Y_S,R_S,h_4^Y\rangle\in L_4$，若等式 $g^U=(X_SY_SP_{Pub}^{h_1})^{h_4^X}R_S^{h_4^Y}$成立，则返回 m 给$\mathcal{A}_{\mathrm{I\text{-}2}}$，否则$\mathcal{F}$停止模拟，并终止；

③若列表 L_{PK}中不存在元组$\langle ID_S,X_S,Y_S\rangle$(即公钥被替换)，当$\langle ID_S,X_S',Y_S',h_1\rangle\in L_1$，$\langle ID_S,R_S,C,h_2\rangle\in L_2$，$\langle ID_S,m_S,X_S',R_S,h_4^X\rangle\in L_4$和$\langle ID_S,m_S,Y_S',R_S,h_4^Y\rangle\in L_4$，若等式 $g^U=(X_S'Y_S'P_{Pub}^{h_1})^{h_4^X}R_S^{h_4^Y}$成立，则返回 m 给$\mathcal{A}_{\mathrm{I\text{-}2}}$，否则$\mathcal{F}$停止模拟，并终止.

伪造：询问阶段结束后，$\mathcal{A}_{\mathrm{I\text{-}2}}$选取随机数 $r\in Z_q^*$，并计算 $R=g^r$；选取满足等式 $g^U=(X_SY_SP_{Pub}^{h_1^S})^{d'}R^{f'}$(其中 $d'=H_4(ID_S,m,X_S,R)$，$f'=H_4(ID_S,m,Y_S,R)$)的随机数 $U\in Z_q^*$；选取满足等式 $V=R^{(x_R+y_R)}$的随机数 $V^*\in Z_p^*$；计算 $C=(m\parallel U)\oplus H_3(V)$ $(f\leftarrow\{0,1\})$和 $h=H_2(ID_S,R,C)$；选取满足 $R=(X_SY_SP_{Pub}^{h_1^S}g^h)^S$的随机数 $S\in Z_p^*$；$\mathcal{A}_{\mathrm{I\text{-}2}}$输出对身份 ID_S和消息 m 的伪造签名$\sigma=(h,S,U,m)$，同时$\mathcal{F}$知道被替换的公钥；若$\mathcal{A}_{\mathrm{I\text{-}2}}$伪造签名成功，并且 ID_S在 L_{PK}中对应的元组$\langle ID_S,X_S,Y_S,c_S\rangle$中的 $c_S=1$，算法$\mathcal{F}$则输出 $b=(S^*h_1^S)^{-1}[r-S^*(r_{Know}^1+r_{Know}^2)]$(其中 $S^*=r(r_{Know}^1+r_{Know}^2+bh_1^S)^{-1}$)作为 DL 问题的有效解；否则，$\mathcal{F}$没有解决 DL 问题.

令事件$\mathcal{E}$表示$\mathcal{A}_{\mathrm{I\text{-}2}}$对挑战身份 ID_S未进行私钥生成的询问，即 $Pr[\mathcal{E}]=1-\frac{q_{SK}}{2^k}$；事件$\mathcal{E}'$表示询问阶段$\mathcal{F}$未终止，即 $Pr[\mathcal{E}']=(1-\delta)^{q_S}$；事件$\mathcal{E}''$表示$\mathcal{A}_{\mathrm{I\text{-}2}}$伪造合法签名后$\mathcal{F}$未终止，即 $Pr[\mathcal{E}'']=\delta$；则模拟过程中$\mathcal{F}$不终止的概率为 $Pr[\mathcal{E}\wedge\mathcal{E}'\wedge\mathcal{E}'']=\left(1-\frac{q_{SK}}{2^k}\right)(1-\delta)^{q_S}\delta$，由于 $\delta=\frac{1}{q_S+1}$，当 q_S足够大时，$(1-\delta)^{q_S}$趋向于 e^{-1}(e 是自然对数底数)，因此模拟过程中$\mathcal{F}$不终止的概率至少为$\left(1-\frac{q_{SK}}{2^k}\right)\frac{1}{\mathrm{e}(q_S+1)}$.

综上所述，若$\mathcal{F}$在模拟过程中未终止，并且$\mathcal{A}_{\mathrm{I\text{-}2}}$以不可忽略的优势 ε 攻破本文方案的不可伪造性，$\mathcal{F}$则能以优势 $Adv(\mathcal{F})\geq\left(1-\frac{q_{SK}}{2^k}\right)\frac{\varepsilon}{\mathrm{e}(q_S+1)}$输出 DL 问题的有效解. 证毕.

定理 7. $\mathcal{A}_{\mathrm{II}}$类敌手的不可伪造性. 在随机谕言机模型中，若敌手$\mathcal{A}_{\mathrm{II\text{-}2}}$能以不可忽略的优势 ε 在多项式时间内赢得相关游戏(游戏具体定义详见文献[7])，$\mathcal{A}_{\mathrm{II\text{-}2}}$最多进行 q_S次签密询问和 q_{SK}次私钥生成询问)，算法$\mathcal{F}$则能以不可忽略的优势 $Adv(\mathcal{F})\geq\left(1-\frac{q_{SK}}{2^k}\right)\frac{\varepsilon}{\mathrm{e}(q_S+1)}$(e 是自然对数底数)在多项式时间内解决 DL 困难问题.

证明思路与定理 6 相似，不再赘述.

5.3 密钥托管

本文方案中，KGC 基于用户身份标识 ID_i和公

开参数 X_i 为用户生成部分私钥 y_i 和部分公钥 Y_i. 由于 $X_i=g^{x_i}$，若 KGC 欲通过 X_i 求解用户的秘密值 x_i，则其将面临求解离散对数困难的问题，即 KGC 无法掌握用户私钥 $SK_i=(x_i,y_i)$.

5.4 公开验证性

由于对 $\mathcal{A}_I$ 类敌手不具备不可伪造性，因此文献[11]中的方案不具有公开验证性；而本文的方案中，当签密发送者和密文接收者关于密文的有效性发生争执，需要公开验证发送者身份时，接收者可发送密文消息 $\sigma=(h,S,C=m\|U)$ 及密文发送者的身份标识 ID_a 给任何第 3 方，第 3 方无需密文收发双方的任何私有信息，只需验证等式 $g^U=(X_aY_aP_{Pub}^{h_1^A})^{d'}R'^{f'}$ 和 $h=H_2(ID_a,R',C)$（其中参数 d'，f'，R' 均可由相关公开信息计算得到）是否成立即可，由于本文方案具有不可伪造性，则当上述等式成立时，即表示密文是由用户 ID_a 生成的合法密文.

5.5 不可否认性

由于对 $\mathcal{A}_I$ 类敌手不具备不可伪造性，因此文献[7]中的方案不具有不可否认性；而本文的方案中，由定理 6 和定理 7 可知，该方案对 $\mathcal{A}_I$ 和 $\mathcal{A}_{II}$ 两类敌手均具有不可伪造性，即密文消息是不可伪造的，因此若签密发送者确实生成了签密密文，那么该发送者就不能够进行否认；同时由公开验证性可知，任何第 3 方均可公开验证密文发送者的身份.

5.6 前/后向安全性

本文方案中，即使在某次签密密文的收发过程中，攻击者获得了签密发送者或密文接收者的相关参数，由于密文生成参数是随机选取的，具有较强的新鲜性，因此攻击者无法获知先前的密文及相关参数，则攻击者无法获知已发送的明文消息；同时，攻击者也无法猜测发送者即将发送的签密密文及其相关参数，因此无法获知将来要发送的明文消息.

6 性能分析

本节将从安全属性、通信开销和计算效率 3 个方面综合分析本文方案和相关无证书签密方案[4-17]的性能，并给出具体的性能对比结果.

由于双线性映射的计算量较大[14]，因此相较于现有的使用双线性映射的无证书签密方案[4-5]而言，不使用双线性映射的签密方案具有更大的效率优势；并且文献[4-5]的方案都存在着安全性缺陷，这些方案要么安全性未进行形式化证明[4]，要么无机密性[5]，所以与使用双线性映射的无证书签密方案相比，本文的方案在效率和安全性方面有明显的优势.

与不使用双线性映射的无证书签密方案[7-12]进行比较时，计算开销主要取决于签密和签密验证算法的计算量，且主要统计群上的点乘运算和指数运算的执行次数，但未统计可提前准备的相关计算；通信开销主要通过密文的长度来衡量；而安全属性主要讨论方案的不可伪造性和机密性.

表 1 中相关符号的含义为：E 表示群上的点乘运算；Q 表示群上的指数运算；$|m|$ 表示明文消息 m 的长度；$|G|$ 表示群 Z_p^* 上相应元素的长度；$|Z_q^*|$ 表示 Z_q^* 上相应元素的长度.

表 1 与不使用双线性映射的相关方案的比较结果

签密方案	计算效率		通信开销	安全属性					
	签密阶段	解签密阶段	密文长度	不可伪造性	机密性	公开验证性	不可否认性	前/后向安全性	密钥托管
文献[7]	$3Q$	$5Q$	$\|m\|+2\|Z_q^*\|$	×	×	×	×	√	√
文献[8]	$3E$	$3E$	$\|m\|+2\|Z_q^*\|$	×	×	×	×	√	√
文献[9]	$3E$	$3E$	$\|m\|+2\|Z_q^*\|$	√	×	√	√	√	√
文献[10]	$3Q$	$3Q$	$\|m\|+\|Z_q^*\|+\|G\|$	√	×	×	√	√	√
文献[11]	$5E$	$6E$	$\|m\|+\|Z_q^*\|+2\|G\|$	√	√	√	√	√	√
文献[12]	$5Q$	$7Q$	$\|m\|+2\|G\|$	√	√	√	√	√	√
本文方案	$2Q$	$4Q$	$\|m\|+3\|Z_q^*\|$	√	√	√	√	√	√

注：√ 表示方案具有该安全属性；× 表示方案不具有该安全属性.

如表 1 所示，在安全性方面，文献[7-10]中方案均存在安全性缺陷，其中本文通过构造具体的攻击算法证明了文献[7]的方案无法满足其所声称的不可伪造性和机密性；基于对文献[8-10]中方案的具体分析，我们发现使用本文的机密性攻击算法可证明文献[8-10]中的方案同样不满足机密性；同时，文献[9]指出文献[8]中的方案对 $\mathcal{A}_I$ 类敌手同样不具备其所声称的不可伪造性. 在计算效率方面，由于文献[11-12]的运算量较大，导致计算效率较低. 在通信开销方面，由于文献[11]的密文较长（表 1 的密文长

度并未统计密文中的代理授权部分)，导致传输代价较大，而其他方案[7-10,12]和本文方案的传输效率较高.

综上所述，现有的不使用双线性映射的无证书签密方案[7-12]在计算效率或安全性方面存在着一定的不足，相比于上述方案，本文方案的计算效率和通信开销以及安全性更优.

7 讨　论

为了满足隐私保护的需求，通信过程中用户通常会对发送的通信消息进行加密和签名操作，以保护通信消息的秘密性和可验证性；用户也可使用签密操作同时完成对通信消息的加密和签名. 由于相比于传统签密方案[7-12]，本文方案在计算效率、通信开销和安全性等方面的性能更佳，因此，本文方案在实际数据传输中有着重要的意义. 文献[15]基于签密方案对移动互联网匿名通信协议进行了相关研究. 由于篇幅所限，对其具体的通信过程，本文不再赘述.

8 结束语

本文通过构造具体的攻击算法证明了文献[7]中的原有方案不具备其所声称的机密性和不可伪造性；同时本文提出了安全高效的无证书签密方案，并在随机谕言机模型下基于 CDH 和 DL 困难问题证明了本文方案的机密性和不可伪造性；由分析可知除上述安全属性之外，本文方案还具有不可否认、公开验证等安全属性. 与现有的传统方案相比，本文方案的计算效率和通信开销以及安全性更优.

致　谢　评审专家及编辑老师对稿件进行了细致的审阅，在此致谢！

参　考　文　献

[1] Zheng Yu-Liang. Digital signcryption or how to achieve cost (signature and encryption)≤cost(signature)+cost(encryption)//Proceedings of the 17th Annual International Cryptology Conference. Santa Barbara, USA, 1997: 165-179

[2] Al-Riyami S S, Paterson K G. Certificateless public key cryptography//Proceedings of the 9th International Conference on the Theory and Application of Cryptology and Information Security. Taipei, China, 2003: 452-473

[3] Shamir A. Identity-based cryptosystems and signature schemes//Blakley G R, Chaum D eds. Advances in Cryptology-Crypto 84. Berlin: Springer-Verlag, 1984: 47-53

[4] Barbosa M, Farshim P. Certificateless signcryption//Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security. New York, USA, 2008: 369-372

[5] Wu Chen-Huang, Chen Zhi-Xiong. A new efficient certificateless signcryption scheme//Proceedings of the Information Science and Engineering, International Symposium on IEEE. Shanghai, China, 2008: 661-664

[6] Li Fa-Gen, Masaaki S, Tsuyoshi T. Certificateless hybrid signcryption//Proceedings of the 5th International Conference (ISPEC 2009). Xi'an, China, 2009: 112-123

[7] Zhu Hui, Li Hui, Wang Yu-Ming. Certificateless signcryption scheme without pairing. Journal of Computer Research and Development, 2010, 47(9): 1587-1594(in Chinese)
(朱辉，李晖，王育民. 不使用双线性映射的无证书签密方案. 计算机研究与发展，2010，47(9)：1587-1594)

[8] Liu Wen-Hao, Xu Chun-Xiang. Certificateless signcryption scheme without bilinear pairing. Journal of Software, 2011, 22(8): 1918-1926(in Chinese)
(刘文浩，许春香. 无双线性配对的无证书签密方案. 软件学报，2011，22(8)：1918-1926)

[9] He De-Biao. Security analysis of a certificateless signcryption scheme. Journal of Software, 2013, 24(3): 618-622 (in Chinese)
(何德彪. 无证书签密机制的安全性分析. 软件学报，2013，24(3)：618-622)

[10] Jing Xiao-Fei. Provably secure certificateless signcryption scheme without pairing//Proceedings of the Electronic and Mechanical Engineering and Information Technology, International Conference on IEEE. Harbin, China, 2011: 4753-4756

[11] Qi Yan-Feng, Tang Chun-Ming, Lou Yu, et al. Certificateless proxy identity-based signcryption scheme without bilinear pairings. China Communications, 2013, 22(11): 37-41

[12] Selvi S S D, Vivek S S, Rangan C P. Cryptanalysis of certificateless signcryption schemes and an efficient construction without pairing//Proceedings of the 5th International Conference Information Security and Cryptology. Beijing, China, 2011: 75-92

[13] Huang Qiong, Wong D S. Generic certificateless encryption in the standard model//Proceedings of the 2nd International Workshop on Security. Nara, Japan, 2007: 278- 291

[14] Chen Li-Qun, Cheng Zhao-Hui, Smart N P. Identity-based key agreement protocols from pairings. Journal of Information Security, 2007, 6(4): 213-241

[15] Zhou Yan-Wei, Wu Zhen-Qiang, Qiao Zi-Rui. Trusted anonymity communication protocol for mobile Internet. Journal of Computer Applications, 2010, 30(10): 2669-2671, 2676(in Chinese)
(周彦伟，吴振强，乔子芮. 移动互联网可信匿名通信模型. 计算机应用，2010，30(10)：2669-2671，2676)

ZHOU Yan-Wei, born in 1986, Ph. D. candidate. His research interests include cryptography and wireless network communication.

YANG Bo, born in 1963, Ph. D., professor, Ph. D. supervisor. His research interests include information security and cryptography.

ZHANG Wen-Zheng, born in 1966, professor. His research interest is information security.

Background

Signcryption is a cryptographic primitive that provides both authenticity and confidentiality with a very low computational cost when compared with the signing and encrypting of a message independently, and it is designed and used to solve the security problem of the information transmitted on the insecure channel. Because the certificateless cryptosystem could reduce the trust on the private key generator, it has become a new research focus in the field of information security.

By using the discrete logarithm and computational Diffie-Hellman, a new method to construct the certificateless signcryption scheme without using the bilinear pairings is proposed in this paper. The scheme is provably secure in the ROM under the CDH and DL assumption. Compared with other existing certificateless signcryption schemes in the computational complexity, the proposed scheme without using bilinear pairing operation, so which has more efficient and security.

This research was supported by the National Natural Science Foundation of China under Grant Nos. 61272436, 61402275, 61572303 and 61303092. The NSFC projects were researched on the theory, application, roaming authentication technology, CK security and anonymous communication in trusted Mobile Internet. The team has published several research articles about anonymous communication, trusted computing, internet of things and cryptography, submitted three industry specifications for trusted digital home, and registered five computer software copyrights.